Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1. (Currently Amended): A method of detecting a rogue access point by a client comprising the steps of:

directing a ~~packet~~ message from the client node to a network through a first access point, the first access point configured to exchange wireless signals with the client node to communicatively couple the client node to the network, to an authentication server, disposed on the network, the message containing identity credentials;

receiving a network response packet by the client node from the first access point responsive to directing a message from the client to a network through a first access point;

determining that the first access point is a rogue access point by the client node based on the network response packet received from the access point in being in nonconformity with predetermined expectations;

sending a start message from the client node to a second access point, the second access point configured to exchange wireless signals with the client node to communicatively couple the client node to the network;

sending an identity request message from the second access point to the client node responsive to the sending a start message;

forwarding the identity response message from the second access point to the authentication server;

validating the identity credentials by the authentication server;

forwarding a send key from the authentication server to the client node through the second access point, the send key comprising key length and key index to specify encryption parameters for a session key;

~~authenticating the client through a valid access point to the network subsequent to determining that the first access point is a rogue access point~~; and

reporting the first access point as a rogue access point by the client node to the network through the valid access point;

wherein the message reporting the first access point as a rogue access point is encrypted with the session key.

Claims 2 - 4 (Cancelled) .

5. (Previously Presented): The method of claim 1 wherein the predetermined expectations comprise data traffic conforming with Institute of Electrical and Electronic Engineers 802.1X standards.

6. (Previously Presented): The method of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein nonconformity is determined by a failure of the mutual authentication.

7. (Previously Presented): The method of claim 6 wherein the mutual authentication comprises:

issuing a challenge from an authentication server to the client node;

issuing a counter-challenge from the client node to the authentication server;

wherein mutual authentication fails at the counter-challenge since the first access point's username and password are not found in the authentication server's database.

8. (Cancelled).

9. (Currently Amended): The method of claim [[8]]1 wherein the identity credentials are a username/password combination.

10. (Cancelled).

11. (Currently Amended): The method of claim 1[[0]] wherein the authentication server is a Remote Authentication Dial-In User Service server and wherein the identity response message is in the form of a Remote Authentication Dial-In User Service access request, wherein the method further comprises the steps of:

responding to the Remote Authentication Dial-In User Service access request with a Remote Authentication Dial-In User Service challenge from the authentication server to the client; and responding from the client to the Remote Authentication Dial-In User Service challenge according to the Remote Authentication Dial-In User Service protocol.

12. (Previously Presented): The method of claim 11 wherein the steps of validating and forwarding comprise sending the client node a Remote Authentication Dial-In User Service accept message and wherein the send key comprises an MicroSoft-Microsoft Point-to-Point Encryption -Send-key.

13. (Cancelled).

14. (Currently Amended): The method of claim 1[[0]] wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

Claims 15 - 20. (Cancelled).

Claim 21. (Currently Amended): A client node configured as a supplicant for detecting a rogue access point comprising:

means for directing a ~~packet~~ message from the supplicant to a network through a first access point, the first access point configured to exchange wireless signals with the client node to communicatively couple the client node to the network, to an authentication server disposed on the network, the message containing identity credentials;

means for receiving a network response packet by the supplicant from the first access point responsive to the means for directing a message from the supplicant to a network through a first access point;

means for determining ~~whether~~ the first access point is a rogue access point based on the network response packet received from the access point being in nonconformity with predetermined expectations;

means for sending a start message from the supplicant to a second access point, the first access point configured to exchange wireless signals with the client node to communicatively couple the client node to the network;

means for sending an identity request message from the second access point to the supplicant responsive to the means for sending a start message;

means for sending an identity response message containing the identity credentials from the supplicant to the second access point in response to the identity request message

means for forwarding the identity response message from the second access point to the authentication server;

means for validating the identity credentials of the supplicant using the authentication server;

means for forwarding a send key from the authentication server to the supplicant through the second access point, the means for forwarding a send key comprises means for supplying key length and key index to specify encryption parameters for a session key;

means for independently deriving a session key from the send key and the identity credentials by the supplicant and the authentication server;

means for encrypting data packets between the supplicant and the authentication server using the derived session key; and

means adapted for reporting the first access point as a rogue access point through [[a]]the second access point that the client is able to authenticate via the means for directing, the means for receiving and the means for determining.

Claims 22-24 (Cancelled).

25. (Previously Presented): The client of claim 21 wherein the predetermined expectations comprise data traffic conforming with Institute of Electrical and Electronic Engineers 802.1X standards.

26. (Previously Presented): The client of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein non-conformity is determined by a failure of the mutual authentication.

27. (Cancelled).

28. (Currently Amended): The client of claim [[27]] wherein the identity credentials are a username/password combination.

29. (Cancelled).

30. (Currently Amended): The client of claim [[29]]21 wherein the authentication server is a Remote Authentication Dial-In User Service server and wherein the identity response message is in the form of a Remote Authentication Dial-In User Service access request, wherein the arrangement further comprises:

means for responding to the Remote Authentication Dial-In User Service access request with a Remote Authentication Dial-In User Service challenge from the authentication server to the supplicant;

and means for responding from the supplicant to the Remote Authentication Dial-In User Service challenge according to the Remote Authentication Dial-In User Service protocol.

31. (Currently Amended): The client of claim [[29]]21 wherein the means for validating and forwarding comprise means for sending the supplicant a Remote Authentication Dial-In User Service accept message and wherein the send key comprises an MicroSoft-Microsoft Point-to-Point Encryption -Send-key.

32. (Cancelled).

33. (Currently Amended): The client of claim [[32]]21 wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

34. (Currently Amended): The client of claim [[27]]21 wherein the supplicant, second access point and authentication server are part of a wireless local area network.

35. (Cancelled).

36. (New) The client of claim 21, wherein means for determining the first access point is a rogue access point is based on a counter-challenge step of a mutual authentication when the username and password of the first access point are not found by the authentication server.

37. (New) The client of claim 21, wherein means for determining the first access point is a rogue access point receives keying material from the authentication server and derives the session key from the keying material and determines a corresponding session key derived by the first access point does not match the session key.

38. (New) A wireless client node, comprising:

a supplicant, the supplicant is configured for authenticating with a first access point, the first access point configured to exchange wireless signals with the client node to communicatively couple the client node to a network, and upon successful authentication with the first access point, the supplicant is configured to issue a counter-challenge to the first access point;

the supplicant is responsive to receiving a response to the counter-challenge from the first access point to determine the response to the counter-challenge is invalid;

the supplicant responsive to determining the response to the counter-challenge is invalid to authenticate with a second access point configured to exchange wireless signals with the client node to communicatively couple the client node to the network, the supplicant sending an identity response message responsive to an identity request message received from the second access point;

the supplicant responsive to receiving keying material from the second access point, the keying material comprising a key length and key index to specify encryption parameters for a session key to derive the session key;

the supplicant responsive to deriving the session key to issue a counter-challenge and validate a corresponding session key derived by the access point;

the supplicant responsive to validating the corresponding session key derived by the access point to encrypt packets using the derived session key; and

the supplicant is responsive to validating the corresponding session key to send a message through the second access point reporting the first access point as a rogue access point encrypted using the derived session key.